International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 6, December 2019, pp. 5340~5350
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i6.pp5340-5350

Node activity based trust and reputation estimation approach for secure and QoS routing in MANET

Raghavendar Raju L.[1], C. R. K. Reddy[2]
[1]University College of Engineering, Osmania University, India
[2]Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, India

Article Info

Article history:

ReceivedOct10, 2018
Revised Apr 24, 2019
Accepted Jul 16, 2019

Keywords:

MANET
Node activity
Reputation
Secure routing
Trust

ABSTRACT

Achieving safe and secure communication in MANETs is a key challenge due to its dynamic nature. A number of security studies disclose that reputation management systems are able to be effectual with less overhead. The reputation of a node is calculated by using automated assessment algorithms depend on predefined trust scheme. This paper proposes a Node Activity-based Trust and Reputation estimation (NA-TRE) approach for the security and QoS routing in MANET. NA-TRE aims to find trust estimation and reputation of a node. The NA-TRE approach monitors the activity changes, packet forwarding or dropping in a node to find the status of the node. The various activities of a node like Normal State (NS), Resource Limitation State (RS) and Malicious State (MS) are monitored. This status of a node is helpful in computing trust and reputation. In this paper NA-TRE approach compared with existing protocols AODV, FACE and TMS to evaluate the efficiency of MANET. The experiment results show that 20% increasing of throughput, 10% decrease of overhead and end to end delay.

Corresponding Author:

Raghavendar Raju L.,
Department of Computer Science and Engineering,
Matrusri Engineering College,
16-1-486, Saidabad, Hyderabad-500059, Telangana, India.
Email: lraghavenderraju@gmail.com

1. INTRODUCTION

The development of wireless communication network provides a communication medium between the devices on the fly through constructing a dynamic and ad hoc network as MANET. The entire communication cycle is depend on the on the nodes which constructing the network. Each one of these node acts as a router, but the dynamic and ad hoc nature of the network does not assure of the accomplishment of the communication. It construct dynamic routes in advance for routing, but these route are always prone to routing attacks and intrusion of malicious nodes. Mostly the designed routing protocols are on an assumption that the participating nodes are trustful and reliable. But, the open and ad hoc network environment make this highly vulnerable and unreliable for the secure communication. This vulnerability and unreliable can cause damage or other dishonest practices can deviate from the network performance. Therefore, the creation of reliable communication, especially when nodes rely entirely on safe path co-operation for successful packet transfer to ensure the efficient use of resources in an ad hoc wireless network, is a crucial issue [1-3].

Secure and QoS routing in MANET is highly challenging due to its network characteristics and resources. Designing efficient routing protocols for security and quality requires supporting resources in terms of energy, memory and processing capacity. In MANET node communicate to each other through a hopping mechanism, where each node finds it nodes in their communication range to establish a route to reach the destination node. It is very difficult for a node to retain communication in a mobility nature as

frequent link failure occurs as a node goes out of the communication range. This cause challenging for MANET to have a QoS routing and even to provide secure routing as nodes very frequently leaves and joins the network randomly. Existing secure routing protocols [4,5] mostly designed on encryption methods are incapable to handle the malfunctioning behavior such as selfishness and maliciousness.

Selfishness and maliciousness can be the intentional or unintentional cause of a node. It is very important to identify such behavior in the network to retain the network life longer. Mostly a selfish node aims to disrupt the network activity through propagating a false rumor about the nodes or make himself unreachable and drops the packets receives. Even it try to create congestion in the network through flooding data packets makes a node to dissipate the energy by overloading or denial the packet forwarding. In general the communication procedure is formed to aim the malicious nodes that are able to affect in the form of "congestion", "denial of service", "path fabrication", etc., [2, 6]. It generate certain problems for communication in the existence of such variety of malicious node in the network. However, there is little work to evaluate as per the best of our understanding, the characteristics of the node. Current tasks explain the routes of neighboring nodes depend on node linkage and packet transmitting to remove malicious nodes [6]. But these tasks do not analyze the effect of the node supported on certain actions for the network firmness.

The existing traditional technique determines the selfish and malicious node based on the packet drop. However, this is not always the case since the node may have another cause for the packet losses. Because of such kind of determination in the activity predictions, most of the approaches was penalized or avoided such nodes in the network. This avoidance or punishment lowers the trust level for the node and is removed from the network during a specific period of time, which is a major drawback and problem of the traditional approaches. Even the effect of frequent changing node activity in real communications makes the problem more complex on prediction and isolation such nodes from the network. In the majority of the previous approaches network isolate nodes based on the performance evaluations related to the "data packet forwarding" and "request responses". Such, isolation make a network unstable and very low performance. To overcome these disadvantages of the past approaches, we aim to address this issue by node reputation estimation mechanism [7, 8] to safeguard long-term network stability to accomplish trustworthy and high-throughput. It present Node Activity-based Trust and Reputation estimation (NA-TRE) approach to compute the reputation of the nodes to assess trustworthiness to overcome the secure routing limitation.

Node activity assessment is a strong factor in determining the credibility of a node and its future forecasts reputation. It will provide node security assurance and effective justification mechanism to eliminate the low reputed nodes from malicious nodes to improve the throughput. The main contribution of the proposal is to precisely distinguish between the malicious node and honest node to have a most reputed route for the communication.

The previous study and analysis also showed that changes in node activity have a strong impact on node survival across the network. We proposed a Node Activity-based Trust and Reputation estimation (NA-TRE) approach which provides two estimation mechanisms to simplify the node isolation problems. The paper contributes the following to provide the novelty to the solution,

- It provides a standard model for classifying node activity by specifying it routing procedures and responses independently to complete any communication between the source and the destination.
- Activity prediction problem based on the classification of activity monitoring by the "Semi-Markov process", where each probability of node activity is calculated by monitoring node runtime activity states.

The trustworthiness problem of a node is handled by predicting the probability of activities and its cumulative confidence calculation, as it identifies the reliable and malicious node efficiently.

The following section of this paper is structured as follows. The related works are discussed in Section-2, node activity and reputation estimation approach discussed in section-3, experiment evaluation and result in the analysis in section-4 and final conclusion of the paper in section-5.

2. RELATED WORKS

MANETs distribute the fundamental security objective with most other networks. It determines the similar features and access control as by the other wireless network for the application communication. However, ad hoc networks cannot be a central administration or coordination, as network participants change their relative positions frequently and the network built on the dependence of the co-operation of nodes, these make it harder to achieve the objective of the conventional network functionality [9-11].

The limited resources in terms of power, memory, bandwidth etc., in most mobile devices is the major concern for deploying the advance security model to identify the specific behavior changes and malicious behavior to provide the secure communication in MANET. This makes nodes not to utilize their resources for transmission of packets on the unreliable network, but it discovers its routes through

broadcasting in advance in performing any data communication in MANET. The past studies [12-14] suggest the impact on the quality of the service due to the node selfishness in MANET. Even though malicious activities are diverse for different causes, there may be nodes in MANET that wants to actively attack the network. Since all nodes are element of the routing infrastructure, these attacks can be effortlessly accomplished and cause a lot of damage [15, 16].

In the literature, there are not many mechanisms for node activity prediction. Therefore, unpleasant behavior of the wireless nodes and multiple failures bring new challenges to the survival of ad hoc networks and encourage disclosure of the effects of their effects [13, 17, 18]. Typically, wireless nodes monitor neighbor node activity, such as "packet forwarding, packet dropping, and network links" for successful packet transmission. However, these activities do not define node activity. In [19], the author considered the impacts of the "indirect observation" of the node offensive propagation. Malicious nodes are able to degrade normal nodes trustworthiness through propagating negative messages and at the similar instance it can recover a malicious node trust through broadcasting positive messages. To avoid such false messages detections, direct and indirect evaluation of trust schemes under the recovery plan can reduce the impacting messages [20].

R. Hinge et al. [21] proposed an "opinion-based trust model" that operates based on network attributes. In this explanation, the reliability of the arbitration node can be calculated and the decision on the communication of the specific path can be supported by the estimation of the trust value. Communication in the MANET must be performed through intermediate nodes because of an inadequate radio range. In consequently the malicious nodes be able to connect to the network and destruct the routing procedure. Thus, for a trust assessment process containing at least two values as "negative" and "positive" in the development of discovering for a trusted node. Later obtaining the trust value for the entire node next to the path, you can take a view of the neighboring node and perform a path searching process.

Dhurandher S K. et al.[12] presents a secure communication for MANET routing using trust known as "Friend based Ad hoc routing using Challenges to Establish Security (FACES)". It describe a method for sharing a network of nodes depended on a record of friends to construct a secure network. The friends are rated depended on flourishing data transfer among the other friend nodes in the network.Every one node periodically runs a procedure to get a shared buddy record to construct a friend's node responsibilities. Based on this regular update, it can effortlessly eliminate malicious nodes from the network. This method does not necessitate observation of neighbor transmissions to assess node confidence. The shortcomings of this proposal are the high-end delay because of the challenge of computational overload and the possible impact of the list of entire friends and communication and network steadiness in the case of malicious behavior of friend nodes.

P. Narula et al. [5] presents a "trust-based secure routing mechanism" for multipath routing in MANET. It implements a data cryptography mechanism to provide a secure data packets routing through a low-trusted mode. The mechanism eliminates the malicious nodes effectively to have a secure route. The routing mechanism utilizes the trust levels to avoids malicious and untrustworthy nodes found in the path to the destination. It assigns a range of trust level ranging between -1 to 4 to define the node trust level. A node having 4 as trust will be highly trustable and -1 is lowest trustable. It suggests that the node with higher trustiness is highly reliable and support in achieving high throughput during data routing. The allocation of trust depends on straight surveillance of neighboring nodes and all admire accepted through several node of the network.Every one encrypted packet is separated into four component, each portion being transmit to multiple accessible paths among the source and destination. It explore the "DSR routing protocol" to discover paths from source to destination. The alternative of path trust is estimated supported on the innovative trust policy.

C. E. Xi et al. [22] presented "Trust Management Scheme Based on Activity Feedback (TMS)" in an inconsiderate environment where node density is low, slow-moving nodes cannot effectively exploit opportunities to achieve self-organizing identity authentication and have no opportunity to participate in network routing. However, in an opportunistic network, it does not need to set up complete mutual authentication for each conversation, assuming most of the communication is caused by the forwarding action. Therefore, a new trust management technique (TMS) is proposed based on the information of behavior feedback to supplement the insufficiency of identity authentication. By using "certificate chains" supported on social characteristics, mobile nodes gradually construct up a "local certificate" graph to appreciate the web of "identity trust" relationships. On the other hand, the successor generates an acknowledged feedback packet for each positive action, thus forming a "behavioral trust" relationship for slow-moving nodes. Simulation results demonstrate that will be capable of effectively progress the transfer probability and the reliability reconstruction fraction when there are many damaged nodes by implementing our trust system, and the "trust management system" capable of proficiently search and filter trust nodes for safe delivery in an opportunistic network.

All of these issues and attacks can have a negative impact on ad hoc networks - both in terms of reliability and bandwidth, and in terms of users' trust in network security. Therefore, the security mechanism to achieve the above goals is obviously mandatory for MANET. In this paper, we mainly focus on the prediction of node activity observations on node activity, and the cumulative reputation calculation based on trust means to significantly reduce network overhead.

3. NODE ACTIVITY BASED TRUST AND REPUTATION ESTIMATION

The trust supervision scheme supervise the node identification and the identification of its participating network [9, 12, 23]. As mentioned above, node activity is the key to evaluating node trust. A node can perform positively or negatively in two traditions. However, the reason for this activity may be real or imaginary to undermine the stability of the network.

But to our knowledge, much work has not yet done to assess the activity of node operations. In support of the node connection and packet transmitting activity, most of the previous studies inform the adjacent node to reduce the malignant nodes. But these actions are never analyzed to their extent to judge a node actual state of function. This proposal aims to solve this problem by assessing the node activity and estimate the trust based to enhance network stability.

We recommend a Node Activity-based Trust and Reputation Estimation (NA-TRE) approach for monitoring node activity to assess the nodes status of the activity as Normal (*N*) or Malicious (*M*), and compute the trust and reputation estimation, which facilitates the effective "decision-making method" for the supervision of node reputation automatically for the consistent data delivery in MANET. However, to our knowledge, small effort has been completed to consider the description of the node activities. Figure 1 illustrates the proposed node activity monitoring for Trust and reputation estimation mechanism for secure routing.

The existing mechanisms describe the activity of neighboring nodes supported on node connections and packet forwarding activities to drop malicious nodes. These mechanism are certainly not analysed the impact of node removal over network stability [24, 25]. The NA-TRE approach improvises the network stability through retaining the genuine nodes for longer.

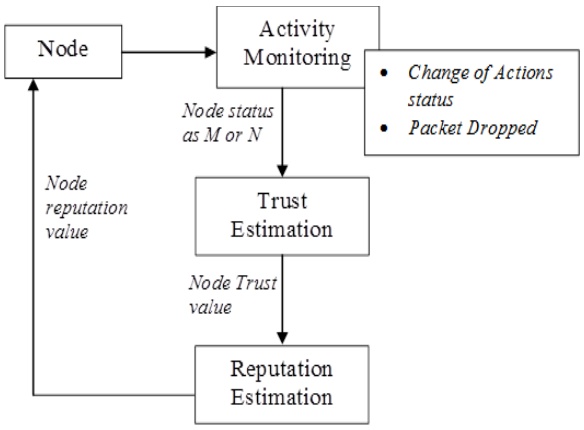

Figure1. NA-TRE mechanism

3.1. Node Activity Monitoring and Trust Estimation

In MANET routing depends on the cooperation of the intermediate nodes and their trust. This is an significant function in MANET that requires maintenance to successfully complete data forwarding [26, 27]. Every node in the network is a separate device and runs on its own system. They are completely independent in determining their behavior and reactions. We monitor these operations for identifying malicious activities based on the supposition that every one nodes in the network behave in the subsequent three operational states:

- *Normal State (NS)*: This state of operation provides the greatest effort for forwarding control and data packets while satisfying all routing regulations and finding the accurate route for well-organized routing.
- *Resource Limitation State (RS)*: This state indicates that it is not supported for network operation Due to "low power consumption", "out of communication range", "high congestion", "frequent link failures", etc.

- *Malicious State (MS):* This state of behavior disrupts routing by initiating "denial of service", "forwarding packet delays", "path creation", and "periodically disseminating positive or negative messages" concerning nodes to provide suspicious activity.

Based on the above actions state inputs node state prediction is performed based on a "Semi-Markov probability decision process" to exactly distinguish the node activity predictions.Let's suppose a network of space *W*, consisting of dissimilar state of nodes as *C* illustrate as "*C = {NS, RS, MS}"*and an activity transforms state in a particular time interval is monitor as *P(t)* which is related to *C*. So, after time *t* the observed in the node activity can be represented as *P(t)* as shown in (1).

$$P(t) = Prob\ (C_{n+1} \rightarrow c_{n+1} \mid C_0 = c_0., \ldots, C_n = c_n) = Prob(C_{n+1} = c_{n+1} \mid C_n = c_n) \quad (1)$$

where, $c_n \in C$, as $c_n$is the element of the collection of node state *C*. The Markov decision chain[28] will be constituted in state *C* using (1) as *{C_n, n = 1, 2 or 3}.* However, the active activity of the node is entirely transformed from one time in the observation chain.

For an illustration, let a node is not supported due to a smaller amount energy levels, then a collection of operations over a period of time may happen to greedy, so the state of action will be resource limitation (RS). This monitoring can conclude a node activity in the present time interval can involve in the future state of action. To have a final state of prediction we considered a set of time interval observation. Let's suppose that a nodes reside for a time, *P(t)* and in the next interval the activity changes from "*P(t)→ $P(t)_i$, i ± 1*"as their other two state changes, and after a period of time interval it has a set of actions changes as "*Z = { $P(t)_1$, $P(t)_2$,$P(t)_1$, $P(t)_3$, . . . }"*. So, to pretend the future probable action state mean, $PA_{mean}$of the collective state changes is computed to decide probable action as given in (2), where if a node in state *NS, RS* is considered as *0 and MS* the considered as 1.

$$PA_{mean} = \frac{\sum Action\ States\ Changes}{No.of\ Interval} \quad (2)$$

Using (2) we find the mean value $PA_{mean}$of each node after a period. If the value $PA_{mean}$is >= S_{TH}, then *"P = M"*, or *"P = N"*, where S_{TH} is the configured state transition threshold and it is assigned 0.6 which means 60% of state changes is identified in a particular period. The S_{TH} value justifies the retaining of a node in a particular state after a period. So, the higher the $_{mean}$ higher the probability of stage change, but to have a limit of PA_{mean}we set the S_{TH} value to 0.6. This prediction of expectations characterization models for the nodes action inference depend on supposition will be self-reliance for suggesting the probable state of action. This predicted *P* state is further utilized to compute the node Trust Estimation (*TE*) of the node in that period using the (3). To have an optimal trust value in case of no change from the normal state we consider a constant of *1/2=0.5* as an addition to the *TE value*, otherwise the reduction trust value as per$\sum M$predicted.

$$TE\ (t) = \int_{i=0}^{t} \frac{\sum N + 1}{\sum N + \sum M + 2} \quad (3)$$

where N-Normal, M-Malicious.

The process of Node Activity Monitoring and Trust Estimation are presented in the Algorithm-1.

Algorithm-1: *Node Activity Monitoring and Trust Estimation Algorithm*

Method: ***NAM_TE(Node n)***
Initialization:
Monitoring time interval, *t = 60 sec*.
Number of interval period, $I_{prd} = 2$;
Estimation time, $E_t = 0$;
Estimation period, $E_{prd} = 0$;
State transition threshold S_{TH} = 0.6
p=0; i=0;

while"*no. of packet to transmit*"***do***
{

```
        E_t =getElapseTime( );
        while (ACK_Time ! = 0 )
        {
                if (RecivedACK =="FWD" )
                        C(t) = "NS";
                else if (RecivedACK =="DoS" ) {
                        FR = findReason( );
                        if (FR = = [BufferOverflow" or "Low Energy"])
                                C(t) = "RS";
                        else
                                C(t) = "MS";
                }
                else if (RecivedACK =="Packet Dropped" )
                C(t) = "RS";
        }
        Z(n)[i ] = C(t); i++;

        //-- Compute Probable Action State
        if (E_t >= t )
        {
                Tot_S_val = 0;
                for (k=0;k <sizeOf (Z) ;k++) {
                        C_v= Z (k);
                if (C_v = = ["NS" or "RS"])
                        S_val = 0;
                else
                        S_val = 1;
                Tot_S_val =Tot_S_val + S_val ;
                }
                PA_mean = Tot_S_val / sizeOf (Z) ;
                if (C_v = = ["NS" or "RS"])
                        P = "M";
                else
                        P= "N";
                A(n)[i ] = P;
                i=0; E_prd++;
        }

        //-- Compute Trust Estimation
        if (E_prd = = I_prd )
        {
                N_val=0, M_val =0 ;
                for (m=0;m<sizeOf(A); m++ ) {
                        V_val= A(m);
                if (V_val = = "N")
                        N_val= N_val+ 1;
                else
                        M_val= M_val+ 1;
                }
                TE = (N_val+ 1)/ (N_val+ N_val +2);
        }
        N_TE (n) [p] = TE;
        p++;
}
```

3.2. Trust based reputation estimation

The computed *TE* using (3) of a node as N_{TE} decides it current node trustworthiness for a period in the communication cycle. As a node have to undergo a different type of transformation state due to the dynamic environment of the network, so it *TE value* also changes accordingly. So, for a complete communication cycle, it may have variation in *TE value* in each set of the period. Let assume a set of *TE valve* for a communication cycle is obtained as, "*Q = {0.4, 0.6, 0.3, 0.8, 0.5}"*, and utilized this variation of *TE value* we can estimate a node reputation as *R* using the (4) given.

$$R = \frac{\sum TE\ Value\ of\ a\ cycle}{Size(Q)} \tag{4}$$

The value of *R* range between *0* and *1*. The minimum *R* threshold value is set to *> 0.6* to retain in the network node else the node will be eliminated. This method of identifying the trusted node supports to build secure and QoS routing for the communication and also provides the fairness to nodes to retain in-network for longer to regain their trustiness. The retaining of the routing nodes in the network supports in achieving network stability and throughput. In the following, section we evaluate this method to justifies the improvisation.

4. EXPERIMENT EVALUATION

In order to evaluate activity monitoring and predictability of trust and reputation, we build this proposed mechanism over the AODV routing protocol. AODV is most stable routing protocol and provides the dynamic routing based on the intermediate node information. The GloMoSim simulator provides a predefined wireless environment framework for the MANET routing. We deploy the developed NA-TRE method in Glomosim to analyze the effectiveness of the proposal. This experiment undertakes to assess the hopeful actions changes of the intermediate node in relative to the number of packets transitions through them to the destination node being transmitted by the source node.

To perform the simulation a wireless environment is configured, where nodes are randomly distributed in a terrain dimension area with others network parameters to support the communication. Data are transmitted in a constant bit rate from the source node to the destination node with a variation of "*0 - 10m/s"* mobility speed. The parameters configured for the simulation are listed in Table1.

Table 1. Simulation configuration parameters

Parameters	Values
Time of the Simulation	*1000s*
Area of Simulation	*1000m X 1000m*
Nodes for Simulation	*100*
Model of Mobility	*RWP*
Mobility Speed	*0 to 20 m/s*
Pause Time	*30s*
Packet Size	*512 bytes*
Data transmit Rate (CBR)	*4pkts/s*
Variation in the Malicious Nodes	*5, 10, 20, 30, 40, 50*

During the simulation, the action of a node changes according to the state of w.r.t. a nodes activity (NS,MS,RS) configured. We considered the packet delivery, link failure and denial of service attributes to predict the probability mean trust over the AODV routing. To analyze the improvisation in the secure routing we compare the NA-TRE approach with "AODV[29]", "FACE [17]" and "TMS [7]".To evaluate the outcome of the simulation we analyze the comparison results of "*Throughput*", "*Packet Dropped*", "*Control Overhead"*and*"End-2-End Delay"*.

4.1. Result analysis

This segment presents the analysis of the results obtained through a varying number of malicious nodes into the network from 5 to 50 numbers for a period 600 seconds simulation having 25 source-destination pairs.

Throughput: Throughput measure the success rate of data packet delivered to the destination node. To provide performance comparison analysis for a better insight of our simulation results, simulation data are presented in Table 2. Figure 2 demonstrate the throughput comparison between the approaches.

All the approaches show above 90% of throughput in the presence of 10 number of the malicious nodes, but with an increasing number of malicious nodes >10 show dropping in throughput. In comparison to the existing approaches the NA-TRE approach show 20% higher throughput.

Table 2. Simulation data for throughput

No. of Malicious Nodes	NA-TRE	AODV	TMS	FACE
5	0.9829095	0.90229095	0.95229095	0.94229095
10	0.968066	0.834066	0.902966	0.919066
20	0.897961	0.6307961	0.814961	0.71307961
30	0.7823182	0.3823182	0.582082	0.53823182
40	0.5506182	0.306182	0.384182	0.38182
50	0.48060472	0.210472	0.3060472	0.3060472

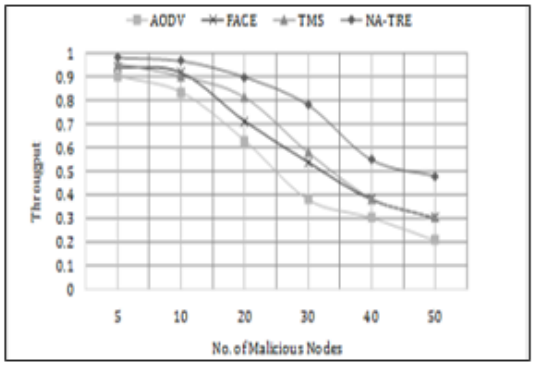

Figure2. Throughput comparison

The effect of the malicious node is examined on a trustworthy node and the measurement of the various parameters is explained here. In Figure 2, shows the throughput is measured. The comparison results show an improvisation over "TMS", "FACE" and "AODV" with different numbers of malicious variations. With the increase, malicious nodes affect the network by dropping packets. As the existing approaches usually penalize all nodes in the action of packet drop, which compromises their trustworthiness even though it's a genuine cause of the loss. NA-TRE instead of punishing every node directly, it monitors each node's activity and its past collected reliability for a period to decide, which helps to allow a genuine node to join back and support in improve throughput and stability for longer.

Control Overhead:The measure of the control overhead compute the network additional processing load in terms of control message exchange for the controlling the communication activities. The simulation results are showed in Table 3. Figure 3 shows the comparison of control overhead between the existing and proposed NA-TRE approach. A difference of an average 15% less number of packet loss is observed compared to the existing approaches, it is due to the trusted and secure route communication. Even the availability of trusted node helps to retain a path for longer to communicate whereas another approach very loses their path due to the malicious activities.

All protocols have achieved significant overhead growth as the number of malicious nodes increase. The AODV has a high overhead for a larger number of malicious nodes, as many data packets are lost and no recovery scenarios can be restored, while FACES, TMS, and the proposed NA-TRE show the difference in control overhead due to maintaining reliable node-based activities prediction. These protocols perform the periodic evaluation of node reliability maintains the safe path and supports in minimizing the packet loss and control overhead.

Table 3. Simulation data for no. of control packets

No. of Malicious Nodes	NA-TRE	AODV	TMS	FACE
5	1163	3156	2057	2154
10	1406	4942	2661	2400
20	3014	6961	4836	5235
30	3552	12467	6946	7961
40	4187	16751	8841	9508
50	5242	21035	11566	15752

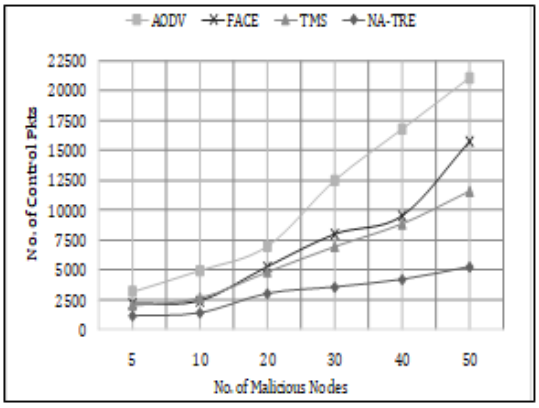

Figure 3.Routing overhead comparison

Number of Packet Dropped: Packet loss or dropped in a network measure the number of denial of service by a node for the request packet transition and simulation results shown in Table 4. Figure 4 shows the comparison packet dropped between the proposed NA-TRE and existing approaches. It shows that with increasing number of malicious node all the approaches have a linear increase in loss packets, but the NA-TRE approaches shows the least among all due to constructing the trusted node route which supports to retain the path for long and smooth data routing to minimize the packet drops.

Table 4. Simulation data for packets dropped

No. of Malicious Nodes	NA-TRE	AODV	TMS	FACE
5	824	1154	1021	1086
10	1250	2856	1298	2005
20	2410	4491	2521	3184
30	2800	6540	3535	5761
40	3980	9912	5298	7820
50	5021	12128	7179	9098

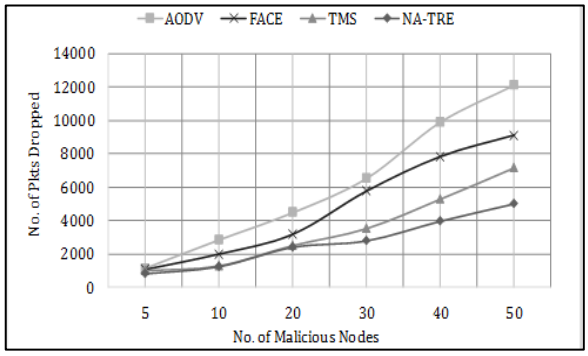

Figure4.Packet drop comparison

End-to-End Delay: It measures the average time taken by a node for data packet delivery and results presented in Table 5. Figure 5 demonstrates the "end-to-end delay" assessment of the proposed NA-TRE and existing approaches. It shows with increasing number of malicious nodes the delay between the ends delivery also increasing. They all show a nearby delay up to 20 number of malicious, but having >20 number of the malicious node the proposed shows 10ms less delay in comparison due to the secure path transmission and the trusted nodes can achieve 99% packet transmission, minimizing the total delay among source and destination nodes.

Improvisation is achieved by identifying the genuine nodes based on its previous activities and performance, rather than punishing nodes on the path as traditional methods, maintaining the network longer and improving performance.

Table 5. Simulation data for the delay

No. of Malicious Nodes	NA-TRE (ms)	AODV (ms)	TMS(ms)	FACE (ms)
5	1.09733	5.42722	1.2523	1.93752
10	3.61966	15.88747	8.83912	11.50053
20	10.95403	22.93019	14.20342	18.7105
30	12.93257	41.80336	29.1018	30.2678
40	20.9468	46.544	31.7263	32.3836
50	21.55	51.3879	38.9205	45.397

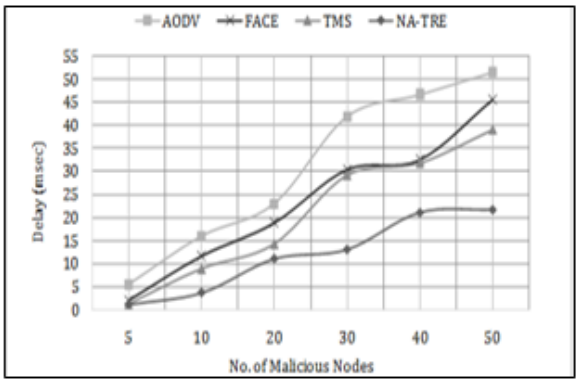

Figure 5.End-to-end delay comparison

5. CONCLUSION

This paper presents a node activity based trust and reputation estimation approach NA-TRE to build a secure and QoS routing in a MANET. The effect of a change in node activity (NS, MS, and RS) during communication resolves the node isolation problem. The proposed NA-TRE approach solves node isolation problem by computing trust and reputation estimation of a node in a network, and malicious prediction. It uses the probabilistic models to calculate the possible node trusts to minimize unfair node isolation. A node trust calculation based on possible node trust improves the node isolation frequency. Experimental results show a 20% improvement of throughput with 10% lowering of the network overhead, packet loss, and end-to-end delay.

In future work, it would enhance this predictive approach by analyzing the transformation in harmful and affirmative messages that transmit trusted and malicious nodes to construct a further stable and secure network. It can also benefit from creating a predictive method by analyzing semantic changes in terms of negative and positive communications published by trusted and malicious nodes to create a more stable network on the network.

REFERENCES

[1] N. Marchang, et al., "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks,"*International Journal of IEEE Transactions on Vehicular Technology*, vol. 66, pp. 1684-1695, 2017.
[2] Z. Movahedi, et al., "Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey,"*International Journal of IEEE Communications Surveys & Tutorials*, vol. 18, pp. 1287-1309, 2016.
[3] M. N. Ahmed, et al., "Flooding Factor based Trust Management Framework for secure data transmission in MANETs,"*J. King Saud Univiversity Com. Inf. Sci*., vol. 29, pp. 269-280, 2017.
[4] J.H.Cho, et al., "Trust threshold based public key management in mobile ad hoc networks,"*Elsevier Ad Hoc Networking*,vol. 44, pp. 58-75, 2016.
[5] P. Narula, et al., "Security in mobile ad-hoc networks using soft encryption and trust based multipath routing,"*International Journal of Science Direct Computer Communication*, vol. 31, 2008.
[6] K. A. B. Ahmed, et al., "A Survey on Trust-Based Detection and Isolation of Malicious Nodes In Ad-Hoc and Sensor Networks,"*International Journal of Frontiers of Computer Science*, vol. 9, pp. 280-296, 2015.

[7] T. Zia, "Reputation-based trust management in wireless sensor networks,"*Proc. International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pp. 163-166, 2008.
[8] Y. Chae, "Redeemable reputation based secure routing protocol for wireless sensor networks," Master of Science Department Computer, University Rhode Island, Tech. Rep. TR12-331, 2012.
[9] M. S. Pathan, et al., "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs,"*Future Internet*, vol. 10, 2018.
[10] T. Shu and M. Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks,"*International Journal of IEEE Transactions On Mobile Computing*, vol. 14, 2015.
[11] W. Li, et al., "Smart: An SVM-based misbehavior detection and trust management framework for mobile ad hoc networks,"*Proc. of International Conf. on Military Communications*, pp. 1102-1107, 2010.
[12] Dhurandher S. K., et al., "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems,"*IEEE Systems Journal*, vol. 5, 2011.
[13] K. Ullah, et al., "Trusted and secured routing in MANET: An improved approach,"*International Journal of IEEE Symposium on Advanced Com. and Comm.*, pp. 297-302, 2015.
[14] M. Li, et al., "MAC-Layer Selfish Misbehaviour in IEEE 802.11 Ad Hoc Networks: Detection and Defence,"*IEEE Trans. On Mobile Comp.*, vol. 14, 2015.
[15] X. Mao and J. McNair, "Effect of on/off misbehavior on overhearing based cooperation scheme for MANET,"*Proc. of International Conf. on Military Communication*, pp. 1086-109, 2010.
[16] N. Marchang and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks,"*International Journal of IET Information Security*, vol. 6, pp. 77-83, 2012.
[17] Z. Wei, et al., "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning,"*IEEE Transactions On Vehicular Technology*, vol. 63, 2014.
[18] T. Jenitha and P. Jayashree, "Distributed Trust Node Selection for Secure Group Communication in MANET,"*Proc. of International Conf. on IEEE 4th Advances in Computing and Communications*, 2014.
[19] T. Shu and M. Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks,"*International Journal of IEEE Trans. On Mobile Comp.*, vol. 14, 2015.
[20] R. A. Shaikh, et al., "Group-based trust management scheme for clustered wireless sensor networks,"*International Journal of IEEE Transaction Parallel Distributed System*, vol. 20, pp. 1698-1712, 2009.
[21] R. Hinge and J. Dubey, "Opinion based trusted AODV routing protocol for MANET,"*Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS), ACM: New York, NY, USA*, 2016.
[22] C. E. Xi, et al., "A Trust Management Scheme Based on Activity Feedback for Opportunistic Networks,"*Network Technology and App. in China Comm.*, 2015.
[23] A. Khana, et al., "A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks,"*Elsevier Future Generation Computer Systems*, vol. 68, pp. 416-427, 2016.
[24] J. Lopez, et al., "Trust management systems for wireless sensor networks: Best practices,"*International Journal of Computer. Communication*, vol. 33, pp. 1086-1093, 2010.
[25] H. Xia, et al., "A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules," *Proc. IEEE/ACM Green Computer Communication*, 2011.
[26] T. Zahariadis, et al., "A novel trust-aware geographical routing scheme for wireless sensor networks,"*International Journal of Wireless personal communications*, vol. 69, pp. 805-826, 2013.
[27] J. Wang, et al., "Building a trusted route in a mobile ad hoc network considering communication reliability and path length,"*International Journal of Network Computer Application*, vol.34, pp. 1138-1149, 2011.
[28] B.J. Chang and S.L. Kuo, "Markov chain trust model for trust value analysis and key management in distributed multicast MANETs,"*IEEE Trans. Vehicular Technol.*, vol. 58, pp. 1846-1863, 2009.
[29] A. Perkins, et al., "Ad-hoc On-Demand Distance Vector (AODV) routing,"*Mobile Ad hoc Networking Working Group Internet draft*, vol. 5, pp. 32-34, 2003.